REMARKS:

Claims 1-29 were presented for examination and were pending in this application. In an Official Action dated August 2, 2004, claims 1-29 were rejected. Applicants thank Examiner for examination of the claims pending in this application and addresses Examiner's comments below. Further, on September 28, 2004, Examiner Tran conducted a telephonic interview with Applicants' representative. Applicants thank Examiner for taking the time to discuss the application with Applicants and include the substance of the interview in the following remarks.

Applicants herein amend claims 1, 2, 6, 7, 8, 13, 17, 18, 21, 24, 25, 27 and cancel claims 11 and 12. Based on the above Amendments and the following Remarks, Applicants respectfully request that Examiner reconsider all outstanding objections and rejections, and withdraw them.

Response to Rejection Under 35 USC 102(e)

In the 4th paragraph of the Office Action, Examiner rejects claims 1-29 under 35 USC § 102(e) as allegedly being anticipated by U.S. Patent No. 6,473,800 to Jerger et al. ("Jerger"). This rejection is now traversed.

During the Examiner interview, Applicants discussed claims 1, 2, and 7 in view of Jerger. As suggested by Examiner during the interview, the claims have been amended to provide more detail. Applicants have amended claims 1, 2, 6, 7, 8, 13, 17, 18, 21, 24, 25, 27 to now recite rules

> for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present.

As discussed with Examiner, known network security properties of a network resource, (e.g., known "backdoors") are defined collectively by conditions present in the network resource. The rules can determine whether the network resource satisfies the conditions and thus whether the resource has the known network security properties.

These claimed rules allow an Intrusion Detection System (IDS) to detect and adapt to changes in the network environment without human intervention. In turn this adaptability allows levels of speed, efficiency, and accuracy to be attained that previously had been regarded as unachievable.

Applicants respectfully submit that the method of Jerger fails to teach or disclose the claimed rules, which are for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present. The method of Jerger simply includes:

> configuring a system security policy to establish multiple security zones, each security zone corresponding to a set of locations on a computer network. Each zone has a corresponding security configuration that specifies the actions to be taken when a protected operation is requested by active content downloaded from that security zone.

Jerger, col. 3, lines 9-16 (3:9-16). In the Jerger method, the security zones are predefined or configured by the user and the security configuration for each zone is also pre-configured as a set of security policy options (e.g., high, medium, low). Jerger at 3:63-4:12. According to Jerger, once a remote location (e.g., the network location being browsed) is recognized as corresponding to one of the pre-defined security zones, a security policy is applied in the local computer with respect to active content downloaded from the remote location.

By contrast, the claimed invention provides rules to determine the presence of conditions in one network resource and the presence of those conditions reveal network security characteristics of that network resource that are generally known, e.g., "backdoors," discrepancies in program code, and the like. In the method of Jerger, the only determination performed is whether a browsed network location or system belongs to a security zone. Based on that determination, a security policy is applied in the local computer with respect to downloaded active content from the browsed location or system. The determination of whether a browsed location belongs to a security zone, even if this were a condition, does not define a known network security characteristic of that browsed location or system. This determination simply causes a predetermined security policy in the local computer to be applied with respect to the downloaded content. Accordingly, in the Jerger method there aren't any rules for determining the presence of conditions in a network resource that collectively define known network security properties of the network resource in which the conditions are present. Therefore, Jerger fails to teach or disclosed the claimed rules.

Based on the above Amendments and Remarks, Applicants respectfully submit that for at least these reasons claims 1, 7, 8, 13, 17, 18, 21, 24, 25, 27 and their dependent claims are patentably distinguishable over the cited reference. Therefore, Applicants respectfully request that Examiner reconsider the rejection of claims 1-10 and 13-29, and withdraw it.

Conclusion

In sum, Applicants respectfully submit that claims 1-10 and 13-29, as presented herein, are patentably distinguishable over the cited references. Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
JOHN S. FLOWERS, ET AL.

Date: 12/2/2004 By: _____

Hector J. Ribera, Attorney of Record
Registration No. 54,397
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7192
Fax: (650) 938-5200
E-Mail: hribera@fenwick.com